SOCIAL SCIENCE FOR SCHOOLS

Cyber Security: Head 2 Head Debate

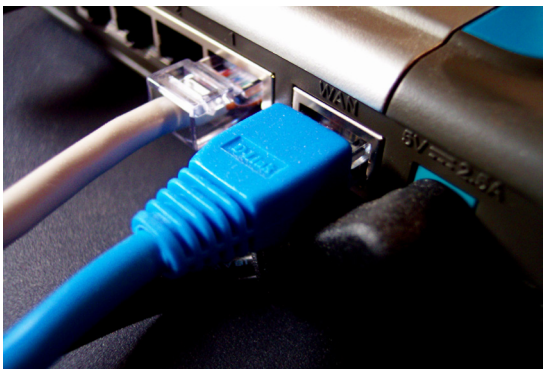
Introduction

The internet has transformed the way we live, work and play. But with the speed and convenience of everything from online shopping to smart government databases come new threats to our security, from extremist websites to virtual identity theft to cyber-espionage and viruses that can crash whole computer systems. Do the risks outweigh the benefits, and what should the balance be between freedom and security online?

The internet as we know it has its origins in the Cold War, with the USA putting money into information technology research in a bid to gain competitive advantage over the Soviet Union, not least for military purposes. It went through various early forms in universities and other institutions before the development of email and at last the World Wide Web in the 1990s. The technology gradually took on a very different culture, owing less to its military and academic origins than a wealth of 'virtual communities' and entrepreneurial businesses who began using and developing the internet early on. Rather than a closed system for the use of governments and universities, the internet became increasingly popular, and infused with an ethos of discovery and openness captured by the slogan, 'Information wants to be free'.

With the new technology, however, came new challenges. The interconnectedness of the internet allowed the possibility of 'hacking', whereby people with sophisticated computer skills could access other people's computers¬ – including those of businesses and government agencies – whether for criminal purposes or simply out of mischief, or indeed more sinister political ends, such as spying for rival governments. This led to the development of a cyber security industry, seeking to come up with ever more watertight systems to protect governments, businesses and individual computer users from attacks. There are other concerns arising from the open and essentially unregulated nature of the internet, however. Since anyone can publish websites and they can be hard to trace, the internet is sometimes used by child pornographers, for example, and indeed supporters of terrorism, arguably posing a serious threat to society.

Police and security services therefore put a lot of resources into monitoring the internet and identifying security threats. But does this undermine the ethos of the internet as a forum for the free exchange of information and ideas? It is not only criminals who would prefer their online activities to remain private, but ordinary users, who often value the internet precisely because it allows them to control what they make public and what they keep private. So is giving up privacy a price worth paying for security? Or should cyber security be about protecting users from official snoopers as well as cyber villains?



This resource has been produced in collaboration with the RCUK Global Uncertainties programme and the Institute of Ideas Debating Matters Competition.